STRATEGY RESEARCH PROJECT

ARTIFICIAL INTELLIGENCE APPLICATIONS TO INFORMATION WARFARE

BY

COLONEL DAVID C. KIRK
United States Army

USAWC CLASS OF 1996

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

ARTIFICIAL INTELLIGENCE APPLICATIONS TO INFORMATION WARFARE

by

Colonel David C. Kirk
United States Army

Dr. Jay Liebowitz
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: David C. Kirk (COL), USA

TITLE: Artificial Intelligence Applications to Information Warfare

FORMAT: Strategy Research Project

DATE: 22 March 1996 PAGES: 32 CLASSIFICATION: Unclassified

In the coming years, a critical element of combat will likely be waged in the information infrastructure. Current strategic concepts do not compensate for the vulnerability of our ever-increasing information-based society. In this research project, artificial intelligence technology (specifically, intelligent agents) was explored. Intelligent agents were found to have characteristics that could help execute an information war. Although there still is work to be done, intelligent agents may someday manage the information flow, be the core technology in network firewalls, and contribute to overall network security through continuous Red Team vulnerability assessments.

1.0 Introduction

The way we think about and respond to information and information infrastructures is profoundly changing the national security interests of this nation. The way the military supports the national security strategy also is changing. The Army, for example, has spent the past four years studying information-age warfare and continues to develop new concepts of battle command, information operations, and command and control warfare.[1] The heart of this change is the computer and computing technologies. Success in information warfare will ultimately go to the nation that can get ahead of the changing technology and develop a national security strategy that harnesses the power of the computer.

A field that is singularly dependent on computer technology is the field of Artificial Intelligence. Recent advances in software devices called "intelligent agents" promise to help shape the future of our information infrastructure.[2]

This paper reviews the challenges of information warfare, explores the technologies of intelligent agents and proposes concepts for intelligent agents in the conduct of information management and information infrastructure security. This paper concludes by presenting recommendations for future research in intelligent agents and in conceptual models for information warfare. Information warfare can be the critical element of the future national security strategy.

2.0 INFORMATION WARFARE

2.1 Definition

Clarity in terminology is more than an academic exercise because the definitions are the basis for policy formulation and it provides a common basis for meaningful discussions. In this paper, definitions are studied because they will help shape the problem and focus the solutions.

None of the past models capture the totality of the concept of information warfare. The most concise synopsis of the evolution of terminology is in COL Fredericks' Information Warfare at the Three Year Mark, Where Do We Go From Here? (1996). He concluded the definition of information warfare presented by the Defense Science Board in 1994 was the result of the most comprehensive review to date.[3] Information warfare is

> actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our own information and information systems.[4]

Information warfare, though, is not restricted to just a military strategy. COL Fredericks explains that IW is not limited "...to a military conflict, declared or otherwise. IW targets the entire information infrastructure of an adversary - political, economic, and military -- throughout the continuum of operations from peace to war.[5] The Joint Chiefs of Staff also uses "the term information warfare in the broadest sense to encompass all offensive information warfare and defensive information warfare actions."[6]

The military application of IW is Command and Control Warfare (C2W). C2W is attacking an enemy military information infrastructure and defending one's own to get inside the enemy commander's decision loop.[7] One might conclude that civilian infrastructures would be immune from such attacks, but not so. Information warfare targets all aspects of a society's ability to wage war.[8]

Note there is an offensive and defensive component to information warfare. The JCS defined defensive information warfare as "all actions to ensure the availability, confidentiality, and integrity of reliable information vital to national security needs."[9] Although most legislation for the protection and privacy of information apply only to the Federal Government, essential economic and national-security related functions are so automated and so interconnected one cannot separate traditional national security infrastructures from commercial infrastructures. As the Joint Chiefs of Staff point out,

> Government networks are interconnected with commercial networks, which are interconnected with financial networks, which are interconnected with the networks which control the distribution of electrical power, and so on. It is now almost impossible to distinguish where one network ends and another begins in this extensive and complex information infrastructure.[10]

Hence, the security of our nation depends on a secure information infrastructure in the broadest sense of the word. We need a national security strategy that addresses the complexity of future information infrastructures.

2.2 Policy or Strategy

The President's National Security Strategy (1995) of "Engagement and Enlargement" had little to say about an information warfare strategy. The organization of the document acknowledged three of the four elements of a national security strategy; diplomatic, political and military.[11] Information was not mentioned. Yet, the President was aware of the dramatic changes in information technology because he mentioned the information revolution in his address to the U.S. Congress in February 1993.[12] He recognized the dramatic potential of the new information technologies, but national security aspects of our information infrastructure were not addressed.

The National Military Strategy (1995) of "flexible and selective engagement" has only one paragraph devoted to information warfare. According to the Joint Chiefs of Staff our strategy is to "Win the Information War." The military must assure our information systems work and our adversaries don't.[13] This is not a strategy.

COL Fredericks, after a thorough search, concluded "no over-arching national policy exists."[14]

> Clearly there is a definite need for leadership in this area. Information assurance (or defensive IW in DOD terminology) has the potential of emerging as a vital national security interest, but it is intertwined with domestic issues. A more intense focus on resources, policy, and interagency cooperation is needed.[15]

2.3 Environment, Vulnerabilities and Threats

The requirement for a defensive information warfare strategy must be justified on more grounds than theoretical models. There

must be a legitimate vulnerability and a verifiable threat.

The communications system that serves the Department of Defense is the Defense Information Infrastructure (DII). The Defense Information Systems Agency (DISA) is the central manager of the DII and responsible for its protection against attack.[16] The DII is a massive network occupying 14 acres of computer rooms, numerous satellites, and digital networks that could circle the globe 400 times.[17] If this were an isolated communications infrastructure its protection would be challenging enough, but

> about 95% of the military's communications are carried over the public switched networks (PSN). These same networks are shared by individual users, universities, various governmental entities, and private corporations, world-wide.[18]

Unlike past DII architectures that were physically isolated from commercial systems, our defense-related infrastructures have evolved into computer-controlled digital networks that are indistinguishable from the National Information Infrastructure (NII).

The problem becomes even more challenging when you consider the NII is becoming indistinguishable from the Global Information Infrastructure (GII).

> Just as there is a merging of the U.S. civilian and military information networks and technologies, so too are the DII and NII becoming inextricably intertwined with the global information environment. This trend will only intensify over time with the application of rapidly advancing technology.[19]

The Joint Chiefs of Staff noted,

> A news broadcast on CNN, a diplomatic communiqué, and

> a military message ordering the execution of an operation, all depend on the global information infrastructure.[20]

Perhaps the only thing we can say for sure, is the information infrastructures of the future will be vastly different than what we have today. The interdependent nature of all the systems, their nearly unfathomable size and the unrestrained growth all contribute to an inherently vulnerable system.

Still, even if the infrastructures are vulnerable and complex, without a viable threat, there is no need for a defensive strategy. Unfortunately, there are ample examples of the threats to our information infrastructures. In 1988, a software worm was released into the Internet infecting over 6000 host computers worldwide in less than two hours.[21] In 1986 and 1987, a computer science student in Hanover, Germany attacked roughly 450 computers operated by the U.S. military and its contractors gaining access to 30 of them. He allegedly had ties to the Soviet KGB.[22] Between April 1990 and May 1991 computer hackers from the Netherlands penetrated 34 DoD sites.[23] The list goes on.

Our national and defense-related systems are vulnerable and there is a very real threat against them. We need a defensive information warfare strategy.

2.4 Information and Infrastructure Security

Although there is no unified strategy for defensive information warfare, the computer security field has some theoretical foundations, much of it written in the last ten

years, which are useful. Computer security strategies have evolved into two distinct branches that provide qualitatively different solutions to the same problem. The Federal government's approach to computer security comes from its role in protecting the national security. Threats generally come from individuals or organizations who have no legitimate access to the government computers, so denying access and maintaining confidentiality is the government's utmost consideration. The National Research Council concluded,

> national security countermeasures stress prevention of attack, and only secondarily investigation and pursuit of the attackers, since the concept of compensatory or punitive damages is rarely meaningful in a national security context.[24]

On the other hand, the commercial sector has evolved security strategies which stress integrity and availability.

> Private sector countermeasures, however, are frequently oriented toward detection--developing audit trails and other chains of evidence that can be used to pursue attackers in the courts.[25]

Relative to the government sector these security strategies are considerably less well developed. The National Research Council discovered,

> Integrity policies have not been studied as carefully as confidentiality policies, even though some sort of integrity policy governs the operation of every commercial data-processing system. Work in this area (Clark and Wilson, 1987) lags work on confidentiality by about 15 years.[26]

Since the government now depends on commercial information infrastructures, security strategies must balance confidentiality, integrity and availability.

In the past, computer security strategies did not use computers as a tool.[27] As the demand for more balance to security increases, the need to use the computer will increase. The National Research Council observed,

> The security challenge for computer technology is that a computer system may be under attack (e.g., for theft of data) for an indefinite length of time without any noticeable effects, attacks may be disguised or may be executed without clear traces being left, or attacks may be related to seemingly benign events.[28]

Thus, there are no traditional danger signals. We need nontraditional security models and tools that use the computer as the security mechanism. As Paul Merenbloom, vice president at Piper Jaffray noted,

> Internet security will open a lot of eyes to the need for fire walls, but there are probably greater needs within organizations to keep data and networks secure from one another. ...as we peer into the not-too distant future, it's clear that virtual--not physical--network designs and implementations will become more popular.[29]

There has been some work in this area. Teresa Lunt was working on expert systems for data integrity through automated auditing in 1988.[30] There are many software programs that check for viruses. In April 1995 SATAN was released on the Internet. SATAN recognized common networking-related security problems, and reported the problems without actually exploiting them.[31] The latest computer security technology is a network firewall. At least 20 different vendors market firewalls and related products.[32]

Thus, there are conceptual frameworks and rudimentary computer security tools that can be adapted for tomorrow's

environment, but traditional strategies are not keeping pace; they are not taking advantage of the power of the computer. Recent advances in artificial intelligence indicate there are solutions to the challenges of information warfare in the field of artificial intelligence.

3.0 Artificial Intelligence (AI)

3.1 Expert Systems

Artificial intelligence was formally initiated in 1956, when the name was coined, making it one of the newest disciplines.[33] On the whole, artificial intelligence failed to meet initial expectations. Charles Babcock, the technical editor of Computerworld observed,

> Artificial intelligence was a casualty of its own hype in the 1980s. Trumped up as a rival to the human brain, it had a few triumphs and many failures.[34]

Recently, though, there has been a new wave of optimism. Douglas Lenat, president of Cycorp, Inc. and consulting professor of computer science at Stanford stated that he believed artificial intelligence stood on the brink of success.[35] His optimism stems from recent advances in the field of intelligent systems. Stephen E. Cross, the director of the Information Technology Center at Carnegie Mellon University (and formerly at Advanced Research Projects Agency), said in December 1995, "I view intelligent systems as the new frontier..."[36]

Perhaps the best known example of an intelligent system is a knowledge-based system or an expert system. Expert systems are computer systems that emulate the decision-making ability of an

expert. Experts or knowledge engineers program a set of "condition-action" rules. The expert system, when presented with a situation, searches for the appropriate condition and returns the associated response. Expert systems use a programmed knowledge base and inferencing techniques to solve problems.[37]

Expert systems were some of the first systems to receive acclaim within the AI community. The early successes were in the field of diagnostic medicine. Today, expert systems are being used in the military, for example, to help schedule ranges, tracking logistics, maintenance, and training, and in force deployment planning.

Expert systems are not without their problems. They are only as good as the expert or knowledge engineer who programmed them, and "the knowledge of the agent is fixed once and for all."[38] As Lenat points out,

> These so-called expert systems were often right in the specific areas for which they had been built, but they were extremely brittle. Given even a simple problem just slightly beyond their expertise, they would usually get a wrong answer, without any recognition that they were outside their range of competence. ...Furthermore, these programs could not share their knowledge.[39]

Sharing knowledge amongst computer systems is one of the newest innovations in expert systems and is a characteristic of a class of intelligent systems called "agents."

3.2 Agents

An agent is anything that perceives its environment through sensors and acts upon that environment through effectors.[40] Although an expert system may be used as an agent, the term

"agent" implies a much more complex structure.

Russell and Norvig (1995), discussing rational agents, highlight a dependency on four things: a performance measure that defines success, a perceptual history of everything the agent has sensed, the agent's knowledge of the environment, and the range of actions the agent can perform.[41] This leads to a definition of an ideal rational agent:

> For each possible precept sequence, the ideal intelligent agent does whatever action is expected to maximize its performance measure, on the basis of the evidence provided by the percept sequence and whatever built-in knowledge the agent has.[42]

Wooldridge and Jennings in The Knowledge Engineering Review (1995), describe an agent by the properties of autonomy, social ability, reactivity, and pro-activeness. Autonomy refers to operating without the direct intervention of humans.[43] Russell and Norvig (1995) include in autonomy the ability to go beyond the built-in knowledge and to react to the precept sequence.[44] Social ability refers to the ability to interact with humans, as well as other agents. Reactivity means to perceive the environment and respond in a timely fashion to changes that occur in it. Pro-activeness refers to the ability of agents to exhibit goal-directed behavior by taking the initiative.

Cross, in his article in IEEE Expert (1995), using different terminology, characterized agents as taskable (in a natural way to humans), articulate (communicating effectively with humans and other systems), competent (defining problems and applying knowledge to solve those problems), and teachable (learning from

experience--either through mentoring or a discovery process).[45] His properties emphasize the need for agents to respond to the human operator and to operate independently.

Intelligent agents must interact with human users, but more importantly for information warfare applications, intelligent agents must interact with other agents. They must be able to operate without man-machine interface. They must go beyond task orientation and seek to accomplish objectives without being told how to do the task.

Although Cross viewed these systems as the "new frontier," he went on to say,

> ...such systems are at least an order of magnitude more difficult to build than expert systems because of the interdependency and integration required between what we usually view as disparate artificial intelligence techniques and methods.[46]

Yet, there is evidence such systems are on the way to becoming a reality.

Peter Fletcher quoted an artificial intelligence expert Christie Guilfoyle as saying, "By the end of the decade the intelligent agent design model will permeate all information systems."[47] British Telecommunications is reported to be developing intelligent agent software as "customer facing agents", "service agents", and "network agents."[48] These are similar to two classes of intelligent systems that Cross called "intelligent assistants" and "intelligent associates."[49] Assistants or customer facing agents interact with humans. They employ domain-specific communication and problem-solving skills

that are easily understood and extended by a human user. Associates, servicing agents, or network agents initiate problem solving in anticipation of demands. Cross points out that assistants exist today and there are laboratory instances of associate systems.[50]

Pattie Maes, associate professor of media arts and sciences at Massachusetts Institute of Technology and president of Agents Technology, Inc., has been working on intelligent software agents that both assist and entertain.[51] She characterizes intelligent agents as software tools that

> instead of user-initiated interaction via commands and/or direct manipulation, the user is engaged in a cooperative process in which human and computer agents both initiate communication, monitor events and perform tasks.[52]

The agent becomes gradually more effective as it learns the user's interests, habits and preferences, as well as those of the community of agents engaged in similar activities. These agents hide the complexity of difficult tasks, they perform tasks on the user's behalf, they can train the user, they help different users collaborate, and they monitor events and procedures.[53]

Intelligent agents overcome two of the traditional problems with knowledge-based approaches--competency and trust. The intelligent agent gradually learns the activities of user and other agents involved in similar activities. Then the agent recommends to the user actions based on conditions it observes and the sequence of past actions. Hence, the agent becomes as competent as the user and, most importantly, as competent as

those agents within its community. If the agent was initially programmed by a more knowledgeable expert than the user, then the agent can also be a trainer. Competence of user and the agent improve. Furthermore, the user develops trust over time as the intelligent agent and the human user collaborate on problems.[54]

3.3 Criteria for Agents

Maes (1994) presents two conditions that make intelligent agents most effective. First, the software application has to involve repetitive behavior. Without repetitive behavior there is no regularity and the agent observes random behavior. This is no different than training a human being. Students must be presented with consistent behaviors to help them internalize the solution and gain confidence that they, when presented with a similar situation, will respond in a like manner.

Secondly, the repetitive behavior should be potentially different for different users. Without this condition, the knowledge-based approach of more traditional expert systems may result in faster results than the learned behavior of an intelligent agent.[55] Intelligent agents must wait for sufficient examples to occur to infer appropriate actions. Efficiencies accrue as the intelligent agent adapts to many users and other agents.

These conditions, repetitive behavior and multiple users, exist in several fields of information warfare. The next section explores specific activities in which the technology of intelligent agents can be applied.

4.0 Applications of Intelligent Agents to Information Warfare

4.1 Information Management

The military is studying the function of battle command because there is concern that confusion increases as the amount of information grows. Unfortunately, conventional tools using human-computer interaction will not suffice in the next generation.[56] The volume of information is too great, our systems too complex, and the rate at which we must assimilate data too fast for military systems to function in the twenty-first century.

There are some rudimentary products on the market today that may help control the amount of information presented a military commander. Network filters such as the Stanford Information Filtering Tool (SIFT) use content-based filtering to search thousands of messages posted to Usenet newsgroups each day. SIFT reads all the texts and analyzes the contents looking for messages that meet interest criteria a user specifies when subscribing to the service.[57] Another free service, Ringo, looks for similar interests amongst a user's peers and recommends musical artists that the user might enjoy. Ringo requests the user provide a list of musical artists rated numerically, then looks for peer groups of other listeners with similar tastes. Ringo then provides the user with the matching groups' lists of musical artists.[58] AT&T offers an agent on PersonaLink which permits users to send messages to another PersonaLink without knowing the other user's address. The agent is released on the

net to scan the PersonaLink directory, find the address, and deliver the message.[59]

These "agents" are not in the same class as the concept of intelligence agents presented in this paper. Maes has developed some prototype agents at the MIT Media Laboratory that can be useful in managing information. The electronic mail handler Maes developed continuously monitors the actions of the user storing situation-action pairs. When a new situation occurs, either the user prepares a message or a message arrives, the agent compares the situation with its stored situations, predicts an action and provides its suggested action to the user. The agent also provides a confidence level for the recommended action. The user can predetermine a "do-it" threshold and a "tell-me" threshold, so that the agent either alerts the user to the new situation or the agent acts autonomously using the closest situation-action pair in its memory. The distance metric used to determine which situation-action pair to select is a weighted sum of the differences for the features that make up the situation. If the confidence level does not exceed even the "tell-me" threshold, the agent does not make a prediction and it presents the situation unresolved.[60]

News filtering agents are also being studied by Maes. The news filtering agents scan full text articles looking for relevant words and structure information such as author and source. Once an agent has been loaded with an initial word and source list, it starts recommending articles to the user. As

with the previous two intelligent agents, the agent then accepts positive or negative feedback for articles or portions of articles recommended. Through the feedback mechanism, the agent's probability that it will recommend similar articles in the future increases or decreases.[61]

Supplying exactly the right list of key words is difficult. To overcome this challenge Maes starts off with several hundred sorting programs called "retrievers." After working with the retrievers, the user picks the ones which did the best job and creates a mixed agent. In addition, a few random "mutations" are added to some of the lists to make them different from those of the parents.[62]

These concepts show promise for managing the volume information thrust on military commanders. The strength of intelligent agents is that they act on the expected situations, divert the unexpected situations to the human user, and learn from each new situation. Thereby, intelligent agents reduce the volume of information and defer only the "difficult" situations to the user.

4.2 Infrastructure Security

The dramatic increase of networks cited above will bring at least as many security problems.

> Several studies have shown that any new Internet connection is likely to be probed for weaknesses within a few hours of going online. One reason for this is the extent to which such probes can be automated and the large number of them that can be running at once.[63]

While there are a computer-based security tools, like SATAN and

firewalls, none of them are in the class of intelligent agents. The National Research Council's (1991) conclusions are still applicable today. "The lack of direct attention to system security is particularly serious given the ongoing dramatic changes in the technology of computing ... (and) make it necessary to rethink some of the current approaches to security."[64] The Council went on to recommend that "new security mechanisms" and "automated security procedures" needed more work.[65]

4.2.1 Intelligent Agent Firewalls

Firewalls are software and hardware configurations and are "like having a big bouncer at the door"[66] of one's network. They are designed to protect a local area network from the Internet. Firewalls are software filters that deny access or route data based on source or destination addresses or ports.[67] They are programmed based on the access policies of the owners of the network. Firewalls are either exclusionary, passing only that which is specifically allowed, or inclusionary, passing everything except that which is specifically denied.

Using Maes' electronic mail handler, the firewall concept could be extended to an intelligent agent firewall. An organization's security policies would be the initial knowledge base. The intelligent agent firewall could then evolve as missions change, projects are completed, and the 27,000 new homepages are added to the World Wide Web each month.[68] The intelligent agent firewall could adapt to the change by

automatically reviewing requests for access, presenting recommended actions and learning from the administrator's actions. This is a qualitative improvement to existing security concepts.

The concept of isolating a local area network from the Internet can be taken one step further using intelligent agent firewall concepts. The greatest security threat, outside of government, is from unauthorized access by authorized users. This is "a problem which consistently outranks external hacking in all infosecurity surveys."[69] Computer experts are already suggesting that firewalls be used to separate structures within a network. Soliciting situation-action pairs from other intelligent agent firewalls helps defend an organization from attacks on all subsets of the network architecture. Consider an employee whose only authorized access is to the organization's operating network. Security policies and access matrices have not anticipated the need for this employee to have access to financial or payroll network. Should the employee attempt to gain access to other than the operational networks, and if there were firewalls installed internal to the organization, current concepts would simply deny access. Intelligent agent firewalls would note the attempted access, check other network agent firewalls to see if other employee accesses had recently changed, and review their precept sequences to see if there was a pattern to the request for access. If the threshold failed to meet the "do-it" threshold, then access would be denied and the network

administrator alerted with a recommendation as to how to handle the access request.

Intelligent agent firewalls would improve the security of existing networks. They reap the benefits of the knowledge-based concepts, performing the well-defined tasks with the expertise of the expert, and they keep pace with the changing environment.

4.2.2 Intelligent Agent Monitors

Taking the concept of firewalls to a lower level than network and sub-network insulation, one might envision an intelligent agent monitor on every terminating device in a system. Agent monitors would observe user activity learning the habits and the work environment of each operator. Norms for hours of operation, accesses to specific drives or networks, software programs used in the course of one's responsibilities would be noted. Furthermore, operators who perform similar duties, called communities, would work similar norms. Should unusual behavior occur because a user changes work habits or the environment changes, the intelligent agent could alert the security manager.

A user might change working procedures as a result of illegal behavior or due to a change in responsibilities or new additions to the environment. For example, a user might work late for several weeks and use a spread sheet or a data base because of a new project. The user might copy an unusual number of files to the floppy drive to take the work home. The intelligent agent monitor would note the changing work habits and

request assistance from other intelligent agent monitors in the user's community. If everyone in the community was busy, the agent monitor may not alert the security manager and accept the deviations from the norms as part of the changing environment. If there is no similar activity, the agent monitor might alert the security manager. The thresholds depend on the security policies of the organization.

4.2.3 Intelligent Agent Security Assessments

Rather than using a pre-programmed assessment, like SATAN, the concept of an intelligent agent could be applied to a family of assessment agents. Each intelligent agent assessor might focus on a particular kind of vulnerability and learn from the changing environment and other similar assessors. For example, there may be agent assessors for password protection, authentication, access authorizations or firewalls. In terms of Maes' news scanners or "retrievers", these agent assessors would share weaknesses found with other agents of their community. They may even mix at some point to provide a hybrid assessment agent.

Learning from the community is critical to the success of this concept. A weakness identified in one network must be passed on to another assessment agent. This is analogous to virus alerts and virus updates, but it is done without the intervention of a human user. Should one agent assessor find password integrity compromised, this would be shared with all assessing agents and alert messages would be sent to the network

administrator.

There is another benefit from using intelligent agent vulnerability assessments. Red Teams are operators who deliberately, with prior approval, attempt to penetrate systems. They are an important part of DISA's protection program.[70] Since computers do repetitive operations rapidly and efficiently, agent assessors could evaluate the network much more frequently than is done today. Network administrators would have an almost continuous assessment by an adaptive Red Team agent assessor.

4.3 Limitations

The results of the first generation of intelligent agents are encouraging, but there are some significant limitations and open questions. The limitations demand more technical research. The questions demand more thought in conceptual architectures, in legal issues and security policies.

Weld in a recent article in AI Magazine (1995) explored the research opportunities in AI relative to shaping the NII. Much of that research would apply to intelligent agents in information management or defensive information warfare. For example, the application of intelligent agents requires more work in knowledge representation. Because relational database and natural language representations are insufficient, new knowledge representation methods are needed to represent information about all aspects of the world. Learning and adaptation methods for machine learning has made rapid progress pushed by recent technical advances, but basic research in new learning algorithms is likely to have

significant payoff.

Research is needed in reasoning about plans, programs and actions if intelligent agents are to chain services and achieve complex objectives. Plausible reasoning tackles the problem of representing, understanding, and controlling the behavior of agents in the context of incomplete or incorrect information. Research is needed for approximation methods for handling very large network structures and developing models of user preferences. There is work needed in multiagent coordination and collaboration. There are successes in identification of protocols, interagent communication paradigms and languages, and implementation of multiagent systems. The vast number of communicating intelligent agents will challenge scalability of current methods.[71]

Questions that must be given further thought are many and varied. For instance, should an intelligent agent learn bad habits from its user? Should a user or systems administrator be held accountable for the actions of the intelligent agent? There are numerous privacy questions that must be addressed. Is it appropriate to record and store work habits that may not have relevance to the user's performance of the task? Can automated systems provide the necessary protection of personal information? Is it legal for one intelligent agent to share personal information of a user with another intelligent agent?[72] There is certainly much work to be done, but intelligent agent concepts show great promise.

5.0 Summary

Information warfare, includes many of the traditional aspects of warfare, particularly command and control warfare, but it opens many new demands for a national security strategy. Degrading a nation's ability to marshal resources and wage war by attacking information infrastructures has become a reality because of the computer. The computer provides incomprehensible complexity and unimaginable efficiencies, but the computer is also the core of infrastructure vulnerabilities.

Artificial intelligence embraces the power of the computer. Recent advances in intelligent agents overcome the traditional challenges of expert systems of competency and trust. They are powerful tools that when applied to information warfare, will markedly change the strategic concepts of information warfare.

Intelligent agents can help solve the challenge of information overload. Intelligent filters not only reduce the volume of information presented military commanders, but also learn from the user and present likely courses of action. Intelligent agents, using existing computer security paradigms, can provide improved firewalls, more sophisticated network monitors and dynamic Red Team assessments.

Although more work needs to be done, experts in AI see great promise in the new agents. When applied to the field of information warfare, intelligent agents will be a viable element of our future national security strategy.

ENDNOTES

1. Kerry A. Blount, "Wrestling with Information Warfare's 'Dark Side,' Army, February 1996, 9.

2. Daniel S. Weld, ed., "The Role of Intelligent Systems in the National Information Infrastructure," AI Magazine 16 (Fall 1995): 45.

3. Brian Fredericks, Information Warfare At the Three Year Mark, Where Do We Go From Here?, (Carlisle Barracks: USAWC, 1996) 3.

4. U.S. Department of Defense, Defense Science Board, Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield, (Washington: Office of the Under Secretary of Defense for Acquisition & Technology, October 1994), B-2.

5. Fredericks, 7.

6. Joint Chiefs of Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance (Washington: Joint Chiefs of Staff, 4 July 1995): 1-1.

7. Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Publication 3-13 coordination draft, (Washington: Joint Chiefs of Staff, May 1995), I-7.

8. JCS, Command and Control Warfare, I-4.

9. JCS, Information Warfare, 1-1.

10. Ibid., 1-4.

11. The White House, A National Security Strategy of Engagement and Enlargement, (Washington: Government Printing Office, February 1995), 1-33.

12. William Clinton, A New Direction, Speech to the 104th Congress, February 1993, 3.

13. Joint Chiefs of Staff, National Military Strategy (Washington: Joint Chiefs of Staff, 1995), 15.

14. Fredericks, 11.

15. Ibid., 12.

16. Robert L. Ayers, "Practicing Defensive Information Warfare," Proceedings of InfoWarCon 1995, (Carlisle: National Computer Security Association, 1995): H5.

17. Ibid., H7-H10.

18. Ronald Knecht and Ronald A. Grove, "The Information Warfare Challenges of a National Information Infrastructure," Proceedings of InfoWarCon 1995, (Carlisle: National Computer Security Association, 1995): A5.

19. Fredericks, 4.

20. JCS, Command and Control Warfare, I-2.

21. JCS, Information Warfare, 2-7.

22. National Research Council, Computers at Risk: Safe Computing in the Information Age, Washington: National Academy Press, 1991, 62.

23. Jack L. Brock, Computer Security: Hackers Penetrate DoD Computer Systems, testimony before the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, United States Senate, (Washington: Government Accounting Office, 20 November 1991), 1.

24. NRC, 19.

25. Ibid.

26. Ibid., 79.

27. Ibid., 78.

28. Ibid., 15.

29. Paul Merenbloom, "Fire Walls Are Not Only for Separating Corporate Networks from the Internet," Infoworld 17 (16 October 1995): 58.

30. NRC, 88.

31. Wietse Veneman and Dan Farmer, "What SATAN Is," homepage for http://www.cs.ruu.nl/cert-uu/satan.html, last modified 24 April 1995.

32. Peter S. Tippett, "A Note from Our President...," NCSA News, January 1996, 4.

33. Stuart Russell and Peter Norvig, Artificial Intelligence, A Modern Approach (Englewood Cliffs: Prentice-Hall, 1995), 3.

34. Charles Babcock, "AI Gets Smart: Intelligent Tools," Computerworld, 11 July 1994, 6.

35. Douglas Lenat, "Artificial Intelligence, A Crucial Storehouse of Commonsense Knowledge Is Now Taking Shape," Scientific American 273 (September 1995): 80.

36. Stephen E. Cross, "The Rest of Our Name: Intelligent Systems and Their Applications," IEEE Expert 6 (December 1995): 2.

37. George Hluck, "A Short Journey Through the World of Artificial Intelligence," an unpublished paper from the Knowledge Engineering Group, Carlisle Barracks, 27 March 1995, 20.

38. Pattie Maes, "Agents that Reduce Work and Information Overload," Communications of the ACM 37 (July 1994): 32.

39. Lenat, 80-81.

40. Russell and Norvig, 31.

41. Ibid., 33.

42. Ibid.

43. Michael Wooldridge and Nicholas R. Jennings, "Intelligent Agents: Theory and Practice," The Knowledge Engineering Review 10, no.2 (1995): 116-117.

44. Russell and Norvig, 35.

45. Cross, 3.

46. Ibid.

47. Peter Fletcher, "Intelligent Agents Will Have Huge Impact on Software," Electronics 67 (8 August 1994): 2.

48. Ibid.

49. Cross, 3.

50. Ibid.

51. Pattie Maes, "Intelligent Software," Scientific American 273 (September 1995): 86.

52. Maes, "Agents that Reduce Work," 31.

53. Ibid.

54. Ibid., 32.

55. Ibid.

56. Weld, 45.

57. J. Blake Lambert, "Artificial Intelligence," *Omni* 17 (April 1995): 12.

58. Ibid.

59. Roberta Salvador, "What's New in Artificial Intelligence," *Electronic Learning* 14 (January 1995): 14.

60. Maes, "Agents that Reduce Work," 35-37.

61. Ibid, 38.

62. David H. Freedman, "Profiles in Artificial Intelligent," *Omni* 17 (February 1995): 63.

63. Linda Stewart, ed., "Firewalls and Internet Security Conference 96," *NCSA News* 6 (Quarter 3 1995): 10.

64. NRC, 207.

65. Ibid., 209-210.

66. John W. Verity, "Hacker Heaven: So Many Computers, So Few Safeguards," *Business Week*, 26 June 1995, 96.

67. Stephen Cobb, "NCSA Firewall Policy Guide," *NCSA News*, January 1996, 6.

68. Stewart, 10.

69. Cobb, 7.

70. Ayers, H29.

71. Weld, 60.

72. Maes, "Intelligent Software," 86.

BIBLIOGRAPHY

Anthes, Gary H. "Great Expectations." Computerworld 29 (April 3, 1995): 89-90.

Arquilla, John. "The Strategic Implications of Information Dominance." Strategic Review (Summer 1994): 24-30.

Arquilla, John and David Rondfeldt. "Cyberwar is Coming!" Comparative Strategy 12 (Apr-Jun 93): 141-165.

Association of the United States Army. "Information Warfare is Top Priority." AUSA News. November 1995, 10.

Ayers, Robert L. "Practicing Defensive Information Warfare." Proceedings of InfoWarCon 95. Carlisle: National Computer Security Association, 1995.

Babcock, Charles. "AI Gets Smart: Intelligent Tools." Computer World, 11 July 1994, 6.

Blount, Kerry A. "Wrestling with Information Warfare's 'Dark Side'." Army (February 1996), 9-15.

Brock, Jack L. Computer Security: Hackers Penetrate DoD Computer Systems. Testimony to the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, United States Senate. Washington: Government Accounting Office, 1991.

Clinton, William. New Direction. Speech to the 104th Congress, February 1993.

Cobb, Stephen. "NCSA Firewall Policy Guide." NCSA News, January 1996, 6-22.

Cross, Stephen E. "The Rest of Our Name Intelligent Systems and Their Applications." IEEE Expert 6 (December 1995): 2-3.

Fletcher, Peter. "Intelligent Agents Will Have Huge Impact on Software." Electronics 67 (8 August 1994): 2.

Fredericks, Brian, COL. Information Warfare At the Three Year Mark, Where Do We Go From Here? USAWC Strategic Research Project. Carlisle Barracks: USAWC, 1996.

Freedman, David H. "Profiles in Artificial Intelligence." Omni 17 (February 1995): 62-64+.

Gore, Al. National Communications Reform. Speech to the Academy of Television Arts and Sciences, 11 January 1994.

Guerrant, Peter D. (GUERRANT@pentagon-hqdadss.army.mil).

"Information Warfare." Electronic mail message to Deb Nye (nyed@awc1) and forwarded to me by Marlin Burkhart (burkharm@awc1) 19 July 1995.

Hluck, George. "A Short Journey Through the World of Artificial Intelligence." Unpublished paper from the Knowledge Engineering Group, Carlisle Barracks, 27 March 1995.

Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W). Draft version of Joint Publication 3-13. Washington: JCS, 1995.

Joint Chiefs of Staff. Information Warfare Legal, Regulatory, Policy and Organization Considerations for Assurance. Report prepared by Science Applications International Corporation (SAIC). Washington: SAIC, 4 July 1995.

Joint Chiefs of Staff. National Military Strategy. Washington: JCS, 1995.

Kievit, James and Steven Metz. "The Internet Strategist: An Assessment of Online Resources." A draft report of the U.S. Army War College, 22 January 1996.

Knecht, Ronald, and Ronald A. Grove. "The Information Warfare Challenges of a National Information Infrastructure." Proceedings of InfoWarCon 95. Carlisle: National Computer Security Association, 1995.

Lambert, J. Blake. "Artificial Intelligence." Omni 17 (April 1995): 12.

Lenat, Douglas. "Artificial Intelligence, A Crucial Storehouse of Commonsense Knowledge Is Now Taking Shape." Scientific American 273 (September 1995): 80-82.

Lunt, Teresa F. "Automated Audit Trail Analysis and Intrusion Detection: A Survey." Proceedings of the 11th National Computer Security Conference. Baltimore: National Institute of Standards and Technology/National Computer Security Center, 1988.

Maes, Pattie. "Intelligent Software." Scientific American 273 (September 1995): 84-86.

Maes, Pattie. "Agents That Reduce Work and Information Overload." Communications of the ACM 37 (July 1994): 31-40.

McConville, Lester F. Information Warfare-Key to National Power in 2020. Directed Study Project AWC 95. Carlisle Barracks: USAWC, 28 April 1995.

Merenbloom, Paul. "Fire Walls Are Not Only for Separating

Corporate Networks from the Internet." Infoworld 17 (16 October 1995): 58.

Minehart, Robert, NSA Representative to the Science Technology Division, U.S. Army War College. Interview by author, 12 February 1996, Carlisle Barracks, PA.

National Research Council. Computers at Risk: Safe Computing in the Information Age. Washington: National Academy Press, 1991.

Petersen, John. "Information Warfare: The Future." Proceedings of InfoWarCon 95. Carlisle: National Computer Security Association, 1995.

Russell, Stuart, and Peter Norvig. Artificial Intelligence A Modern Approach. Englewood Cliffs: Prentice Hall, 1995.

Salvador, Roberta. "What's New in Artificial Intelligence?" Electronic Learning 14 (January 1995): 14.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Steele, Robert. "National and Corporate Security in the Age of Information." Proceedings of InfoWarCon 95. Carlisle: National Computer Security Association, 1995.

Stein, George J. "Information Warfare." Airpower Journal (Spring 1995): 31-39.

Stewart, Linda, ed. "Firewalls and Internet Security Conference 96." NCSA New 6 (Quarter 3 1995): 10.

Thompson, Mark. "If War Comes Home." Time (August 21, 1995): 44-46.

Tippet, Peter S. "A Note from Our President...." NCSA News, January 1996, 4.

Toffler, Alvin and Heidi. War and Anti-War Survival at the Dawn of the 21st Century. Boston: Little, Brown and Co., 1993.

Toffler, Alvin. The Third Wave. New York: Morrow, 1983.

Turban, Efraim. Expert Systems and Applied Artificial Intelligence. New York: Macmillan Publishing Co., 1992.

U.S. Department of Defense, Defense Science Board. Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield. Washington: Office of the Under Secretary of Defense for Acquisition & Technology, October

1994.

Varian, Hal R. "The Information Economy." Scientific American 273 (September 1995): 200-202.

Verity, John W. "Hacker Heaven: So Many Computers, So Few Safeguards." Business Week, 26 June 1995, 96.

Waller, Douglas. "Onward Cyber Soldiers." Time (August 21, 1995): 38-44.

Weld, Daniel S., ed. "The Role of Intelligent Systems in the National Information Infrastructure." AI Magazine 16 (Fall 1995): 45-64.

White House. A National Security Strategy of Engagement and Enlargement. Washington: Government Printing Office, February 1995.

Wooldridge, Michael, and Nicholas R. Jennings. "Intelligent Agents Theory and Practice." The Knowledge Engineering Review 102 (June 1995): 115-152.